9110-9B

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2020-0005]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of a modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify a current DHS system of records titled, "Department of Homeland Security/ALL-023 Personnel Security Management System of Records." This system of records describes DHS's collection and maintenance of records related to the processing of personnel security-related clearance actions, suitability determinations, fitness determinations, whether security clearances are issued or denied, and the verification of eligibility for access to classified information or assignment to a sensitive position.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified routine uses will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2020-0005 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

- Fax: 202-343-4010.
- Mail: Constantina Kozanas, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2020-0005. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general and privacy questions, please contact: Constantina Kozanas, 202-343-1717, Privacy@hq.dhs.gov, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

The Department of Homeland Security requires certain individuals, such as employees and contractors, to undergo a background investigation prior to being granted access to DHS information and facilities. Some DHS components have delegated authority from the Office of Personnel Management as the Suitability Executive Agent and the Office of the Director of National Intelligence as the Security Executive Agent to conduct their own personnel security investigations. This system of records covers background investigations completed by those DHS components with delegated authority

(e.g., CBP, ICE), and adjudications of background investigations for all DHS personnel.[1] DHS is modifying and reissuing DHS/ALL-023 Personnel Security Management SORN. DHS and its components and offices rely on this SORN for the collection and maintenance of records that pertain to personnel security management. The DHS/ALL-023 Personnel Security Management System of Records is the baseline system for personnel security activities, as led by the DHS Office of the Chief Security Officer, for the Department. DHS is updating the purpose of this SORN to include:

- Adding the use of personnel security records to assess eligibility for Law Enforcement Officers Safety Act (LEOSA) Photographic identification cards.
- Adding the Prison Rape Elimination Act of 2003 (PREA) as an authority for collection.
- Updating the category of individuals to include those individuals who are seeking a credential that requires review of information contained in this system of records.
- Updating the categories of records to include publicly available information, such as information obtained from social media, that may be collected as part of the background investigation process, as described in Office of the Director of National Intelligence (ODNI) Security Executive Agent Directive (SEAD) 5; address and phone number for individuals; polygraph records; fingerprints and fingerprint records; and information about an individual's character reference(s). Additionally, DHS is updating the category of records to include information

[1] Background investigations for all other components are conducted by the Department of Defense and fall under Personnel Vetting Records System, DUSDI 02-DoD, 83 FR 52420 (October 17, 2018).

collected as part of the Department's compliance with the Prison Rape Elimination Act of 2003.

- Modifying routine uses E and F as required by OMB Memorandum M-17-12, modifying routine use J to clarify when DHS may share information from this SORN with a potential or current employer; and adding routine use M to document sharing with the National Counterintelligence and Security Center (NCSC) for the purpose of continuous evaluation.
- Updating the retention schedule to conform to the new General Records Schedule 5.6.

This notice also includes non-substantive changes to simplify the formatting and text of the previously published notice.

Consistent with DHS's information sharing mission, information stored in the DHS/ALL-023 Personnel Management System of Records may be shared with other DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

There will be no change to the Privacy Act exemptions currently in place for this system of records and therefore they remain in effect. This updated system will continue to be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory

framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides covered persons with a statutory right to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/ALL-023 Personnel Security Management System of Records.

In accordance with 5 U.S.C. sec. 552a(r), DHS has provided a report of this system of records to the Office of Management and Budget and to Congress.

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/ALL-023 Personnel Security Management System of Records.

SECURITY CLASSIFICATION: Unclassified and classified.

SYSTEM LOCATION: Records are maintained at several DHS Headquarters locations and component offices in Washington, D.C. and field locations. For records on background investigations maintained and adjudicated by the Office of Personnel Management (OPM) or the Department of Defense's (DoD) Defense Counterintelligence

and Security Agency, OPM or DoD's DCSA may retain copies of those records and files pursuant to their records retention schedules.

SYSTEM MANAGER(S): Enterprise Security Services Division (202-447-5010), Office of the Chief Security Officer, Department of Homeland Security, Washington, D.C. 20528.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 8 U.S.C. 1357(g); 19 U.S.C. 1401(i); Prison Rape Elimination Act of 2003, Pub. L. No. 108–79, 117 Stat. 972 (45 U.S.C. 15601 et seq.); Executive Order (EO) 9397, as amended by EO 13478; EO 10450; EO 12968; EO 13467; EO 13764; EO 13869; 5 CFR 731; 5 CFR 732; 5 CFR 736; Homeland Security Presidential Directive 12; SEAD 2; SEAD 4; SEAD 5; SEAD 6; 6 CFR part 115; and Intelligence Community Directive 704.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to collect and maintain records of processing of personnel security-related clearance actions, to record suitability determinations, fitness determinations, whether security clearances are issued or denied, and to verify eligibility for access to classified information or assignment to a sensitive position. Also, records may be used by the Department for adverse personnel actions such as removal from sensitive duties, removal from employment, denial to a restricted or sensitive area, and revocation of security clearance. The system also assists in capturing background investigations and adjudications; directing the clearance process for granting, suspending, revoking, and denying access to classified information; directing the clearance process for granting, suspending, revoking, and denying other federal, state, local, or foreign law enforcement officers the authority to enforce federal laws on behalf of DHS; managing state, local, tribal, and private sector clearance

programs and contractor fitness programs; determining eligibility for credentials such as the Law Enforcement Officers Safety Act (LEOSA) Photographic identification card; determining eligibility for unescorted access to DHS-owned, DHS-occupied, or DHS-secured facilities or information technology systems; and/or other activities relating to personnel security management responsibilities at DHS.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by this system include federal employees, applicants, excepted service federal employees, contractor employees, retired employees, and past employees providing support to DHS who require or required: 1) unescorted access to DHS-owned facilities, DHS-controlled facilities, DHS-secured facilities, or commercial facilities operating on behalf of DHS; 2) access to DHS information technology (IT) systems and the systems' data; or 3) access to national security information, including classified information.

Also covered are: 1) state, local, and tribal government personnel and private sector individuals who serve on an advisory committee or board sponsored by DHS; 2) federal, state, local, and foreign law enforcement personnel who apply for or are granted authority to enforce federal laws on behalf of DHS; and 3) individuals, including state, local, and tribal government personnel and private sector individuals, who are authorized by DHS to access Departmental facilities, communications security equipment, and/or information technology systems that process sensitive or classified national security information.

CATEGORIES OF RECORDS IN THE SYSTEM:

- Individual's name;

- Individual's address;
- Individual's phone number;
- Date and place of birth;
- Social Security number;
- Citizenship;
- Access Control Pass or Credential number;
- Facial photograph;
- Fingerprints and fingerprint records;
- Polygraph reports, polygraph charts, polygraph tapes, and notes from polygraph interviews or activities related to polygraph interviews;
- Records relating to the management and operation of DHS personnel security programs, including but not limited to:
    - Completed standard form questionnaires such as SF-85, SF-85P, and SF-86;
    - Originals or copies of background investigative reports;
    - For individuals covered by the DHS PREA rule, information related to whether the individual has been convicted of engaging or attempting to engage in sexual activity facilitated by force, overt or implied threats of force, or coercion, or if the victim did not consent or was unable to consent or refuse; or who has been civilly or administratively adjudicated to have engaged in such activity;
    - Supporting documentation related to the background investigations

and adjudications including criminal background, medical, and financial data;

- Documentation related to an individual's character reference(s), including names, addresses, telephone numbers, and statements;
- Publicly available electronic information, including information obtained from social media;
- Information related to congressional inquiry; and
- Other information relating to an individual's eligibility for access to classified or sensitive information.

- Records relating to management and operation of DHS programs to safeguard classified and sensitive but unclassified information, including but not limited to:
  - Document control registries;
  - Courier authorization requests;
  - Non-disclosure agreements;
  - Records of security violations;
  - Records of document transmittals; and
  - Requests for secure storage and communications equipment.
- Records relating to the management and operation of DHS special security programs, including but not limited to:
  - Requests for access to sensitive compartmented information (SCI);
  - Contact with foreign officials and foreign travel registries; and
  - Briefing/debriefing statements for special programs, sensitive

positions, and other related information and documents required in connection with personnel security clearance determinations.

- Records relating to the management and operation of the DHS security program, including but not limited to:
    - Inquiries relating to suspected security violation(s);
    - Recommended remedial actions for possible security violation(s);
    - Reports of investigation regarding security violations;
    - Statements of individuals;
    - Affidavits;
    - Correspondence;
    - Documentation pertaining to investigative or analytical efforts by DHS Security program personnel to identify threats to DHS personnel, property, facilities, and information (e.g., travel records obtained as part of continuous evaluation); and
    - Intelligence reports and database results relating to DHS personnel, applicants, or candidates for DHS employment or access to DHS facilities or information.

RECORD SOURCE CATEGORIES: Records are generated from the individual receiving the background investigation, relevant law enforcement databases, publicly available electronic information, and from sources contacted during personnel and background investigations.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those

disclosures generally permitted under 5 U.S.C. sec. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including the U.S. Attorneys Offices, or other federal agencies conducting litigation or proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity, only when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined

that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to

the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

I. To an appropriate federal, state, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

J. To a prospective or current employer that has, or is likely to have, access to any government facility, information, equipment, network, or system, to the extent necessary to determine the employment eligibility of an individual, based on actions taken by the Department pursuant to a personnel security matter involving the individual.

K. To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations; in connection with criminal law proceedings; or pursuant to the order of a court of competent jurisdiction.

L. To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

M. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

N. To the National Counterintelligence and Security Center (NCSC) to assist in the ongoing review of an individual's eligibility for access to classified information or to hold a sensitive position.

O. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS may be retrieve records by individual's name, date of birth, Social Security number, if applicable, or other unique individual identifier such as access control pass or credential number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Pursuant to GRS 5.6, Items 170 through 200, records relating to persons who were not granted security clearances are destroyed one year after consideration of the candidate ends, but longer retention is authorized if required for business use. Records related to individuals granted a clearance are destroyed five years after employee or contractor relationship ends, but longer retention is authorized if required for business use. Records related to alleged security violations are destroyed five years after closure of case or final action, whichever is sooner, but longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and the Judicial Redress Act if applicable, because it is a law enforcement system. However, DHS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and Chief Freedom of Information Act

(FOIA) Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes the records would have been created; and

- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the requester must include an authorization from the second individual certifying his/her agreement for the requester to access his/her records.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record.

NOTIFICATION PROCEDURES: See "Record Access Procedures" above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(1), (k)(2), (k)(3), and (k)(5), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. sec. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I); and (f).

HISTORY: DHS/ALL-023 Personnel Security Management System of Records, 74 FR 3084 (January 16, 2009), 75 FR 8088 (February 23, 2010); Implementation of Exemptions, DHS/ALL-023 Personnel Security Management System of Records, 74 FR 50904 (October 1, 2009).

Constantina Kozanas,
Chief Privacy Officer,
Department of Homeland Security.

[FR Doc. 2020-22536 Filed: 10/9/2020 8:45 am; Publication Date: 10/13/2020]